

4

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-264595

(43)Date of publication of application : 19.09.2003

(51)Int.Cl.

H04L 12/66

H04L 12/56

(21)Application number : 2002-063993

(71)Applicant : MITSUBISHI ELECTRIC CORP.

(22)Date of filing : 08.03.2002

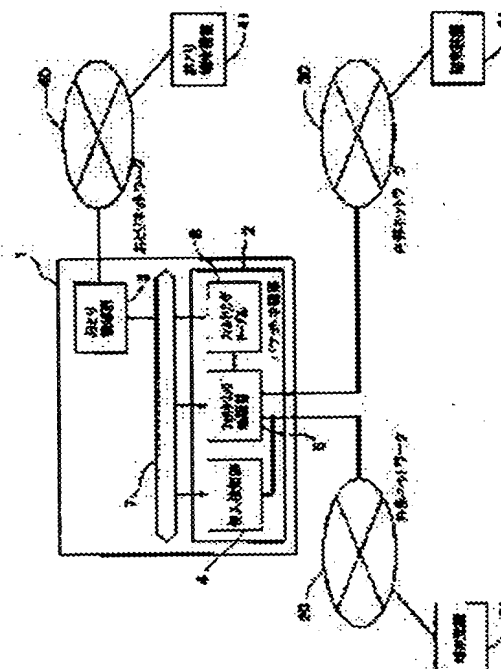
(72)Inventor : KINOSHITA YOSUKE

## (54) PACKET REPEATER DEVICE, PACKET REPEATER SYSTEM, AND DECOY GUIDING SYSTEM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a packet repeater system whose security property against any illegal access is improved by transmitting an illegal access packet or any suspicious packet to a decoy network.

**SOLUTION:** This packet repeater system is provided with a packet relay part 2 for relaying a packet between networks 20 and 30 and a decoy guiding part 3 for transmitting the packet from the network 20 to a decoy network 40. The packet relay part 2 is provided with a filtering part 5 for deciding whether to discard or decoy-guide the packet from the network 20 by using a filtering table 6 and an intrusion detecting part for updating the filtering table 6 by monitoring the packet from the network 20.



## LEGAL STATUS

[Date of request for examination]

06.01.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office



## 【特許請求の範囲】

【請求項 1】 第 1 のネットワークおよび第 2 のネットワーク間でパケットを中継するパケット中継部と、第 1 のネットワークから第 2 のネットワークに対して送信されたパケットを第 1 および第 2 のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを備え、上記パケット中継部が、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、  
フィルタリングテーブルを用いて、第 1 のネットワークから第 2 のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、  
第 1 のネットワークから第 2 のネットワークに対して送信されたパケットを監視して、第 2 のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とを有することを特徴とするパケット中継装置。

【請求項 2】 上記オトリネットワークは、第 2 のネットワークと同一のアドレス体系を有するとともに、オトリ端末装置が接続され、

上記オトリ誘導部は、オトリ誘導されるパケットの送信先アドレス情報に一致する第 1 のアドレス情報が割り当てられたオトリ端末装置に対してパケットを送出することを特徴とする請求項 1 に記載のパケット中継装置。

【請求項 3】 上記侵入検知部は、第 1 のネットワークから第 2 のネットワークに対して送信されたパケットを所定の不正アクセスパケットのパターンデータと比較して、不正アクセスパケットを検出することを特徴とする請求項 1 に記載のパケット中継装置。

【請求項 4】 上記オトリ誘導部は、オトリ端末装置から第 1 のネットワークに対して送信されたパケットをパケット中継部へ送出し、  
パケット中継部は、オトリ端末装置からのパケットを第 1 のネットワークへ送出することを特徴とする請求項 1 又は 2 に記載のパケット中継装置。

【請求項 5】 上記オトリ誘導部は、オトリネットワークに接続された汎用コンピュータにより構成され、その汎用データバスを介してパケット中継部に接続され、  
上記パケット中継部は、オトリ誘導部から受信したオトリネットワークから第 1 のネットワークに対して送信されたパケットに対し、フレーム形式を第 2 のネットワークの形式に変換して第 1 のネットワークに送出することを特徴とする請求項 4 に記載のパケット中継装置。

【請求項 6】 上記オトリ誘導部は、オトリ端末装置から第 1 のネットワークに対して送信されたパケットについて、その送信先情報に基づき、オトリ誘導されたパケットの送信元以外を送信先とするパケットを判別し、判別されたパケットの送信元情報をオトリ端末装置に割り

当てられた第 2 のアドレスに変更してパケット中継部へ送出することを特徴とする請求項 2 に記載のパケット中継装置。

【請求項 7】 上記パケット中継部は、第 1 のネットワークから送信されるパケットについて、第 2 のアドレスを送信先情報とするパケットを判別し、  
上記オトリ誘導部が、判別されたパケットの送信先情報を第 1 のアドレスに変更して、オトリネットワークへ送出することを特徴とする請求項 6 に記載のパケット中継装置。

【請求項 8】 請求項 4 に記載された第 1 および第 2 のパケット中継装置と、パケットを監視するパケット監視装置からなり、  
第 1 のパケット中継装置の第 1 のネットワーク用のポートが第 1 のネットワークに接続され、  
第 2 のパケット中継装置の第 1 のネットワーク用のポートが第 2 のネットワークに接続され、  
第 1 および第 2 のパケット中継装置の第 2 のネットワーク用のポートが互いに接続され、正常パケットが伝送される第 1 の経路を形成し、

第 1 および第 2 のパケット中継装置のオトリネットワーク用のポートが互いに接続され、監視用経路として第 1 のパケット中継装置によってオトリ誘導されるべきパケットが伝送される第 2 の経路を形成し、  
パケット監視装置が第 2 の経路に設けられることを特徴とするパケット中継システム。

【請求項 9】 第 1 のネットワークおよび第 2 のネットワークに接続されたパケット中継装置と、第 1 および第 2 のネットワークとは別のオトリネットワークを介してパケット中継装置に接続されたオトリ端末装置とを備え、

パケット中継装置が、第 1 のネットワークおよび第 2 のネットワーク間でパケットを中継するパケット中継部と、第 1 のネットワークから第 2 のネットワークに対して送信されたパケットを第 1 および第 2 のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを有し、

上記パケット中継部が、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、

フィルタリングテーブルを用いて、第 1 のネットワークから第 2 のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、  
第 1 のネットワークから第 2 のネットワークに対して送信されたパケットを監視して、第 2 のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とを有することを特徴とするオトリ誘導システム。

【請求項 10】 上記パケット中継装置は、第 1 のネッ

トワークから第2のネットワークへの通信量が所定の閾値を越える場合に、第1のネットワークからのパケットをオトリ端末装置へ送出し、

上記オトリ端末装置は、パケット中継装置からの上記パケットを記録し、第1のネットワークから第2のネットワークへの通信量の低減後に第2のネットワークに対し送信することを特徴とする請求項9に記載のオトリ誘導システム。

【請求項11】 上記オトリ端末装置は、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、オトリ誘導されたパケットを第2のネットワーク又は身代わり端末装置に対して送信することを特徴とする請求項9に記載のオトリ誘導システム。

【請求項12】 上記パケット中継装置は、第1のネットワークから第2のネットワークに対して送信されたパケットを第2のネットワークおよびオトリ端末装置へ送出し、

オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、第2ネットワークの監査を行うことを特徴とする請求項9に記載のオトリ誘導システム。

【請求項13】 上記オトリ端末装置は、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、セッションリセットパケットを第1のネットワークに対して送出することを特徴とする請求項9に記載のオトリ誘導システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、パケット中継装置およびオトリ誘導システムに係り、更に詳しくは、侵入検知機能とネットワーク中継機能とを連携させるとともに、外部ネットワークからのパケットをオトリネットワークへ誘導することができるパケット中継装置、並びに、これを用いたパケット中継システムおよびオトリ誘導システムに関する。

【0002】

【従来の技術】図13は、従来の侵入検知システムの構成および動作を示した図である。図中の1はパケット中継装置、20は外部ネットワーク、21は外部端末装置、30は内部ネットワーク、31は内部端末装置、50は管理者端末、51は解析装置である。

【0003】パケット中継装置1は、外部ネットワーク20および内部ネットワーク30に接続され、両ネットワーク間での通信されるパケットの中継を行っている。すなわち、外部端末装置21から内部端末装置31へのパケットを外部ネットワーク20から受信し、内部ネットワーク30へ送出する。また、内部端末装置31から外部端末装置21へのパケットを内部ネットワーク30から受信し、外部ネットワーク20へ送出する。

【0004】ここで、外部ネットワーク20から内部ネ

ットワーク30へのアクセスは制限されている場合がある。例えば、IDコード及びパスワードによって認証された者だけが内部端末装置31にアクセスすることが出来るような場合である。このような場合、外部ネットワーク20から内部ネットワーク30へ不正にアクセスしようとする攻撃者からのパケット、つまり、不正アクセスパケットが送られてくることがある。

【0005】このような不正アクセスから内部ネットワークを防御するため、一般に、パケット中継装置1は、不正アクセスパケットを検出するためのフィルタリング機能を有している。このようなパケット中継装置は、不正アクセスパケットの送信元又は送信先情報が規定されたフィルタリングテーブルを用いて、外部ネットワーク20からの不正アクセスパケットを判別し、不正アクセスパケットであることが判別できれば、当該パケットは内部ネットワーク30へ送出されない。

【0006】このようなフィルタリング機能を有するパケット中継装置においては、フィルタリングテーブルの内容が重要であり、内部ネットワーク30のセキュリティを高めるために、一元的なポリシー（特定のデータを受信すれば通信を遮断する等の極端なポリシー）を設定したとすれば、不正アクセスは排除することができるが、ネットワークの可用性を確保することが困難になる。このため、運用時に、ネットワーク管理者が、不正アクセスの疑いのある被疑パケット1つ1つについて不正アクセスパケットであるか否かを判断し、フィルタリングテーブルを更新していく必要がある。

【0007】解析装置51は、パケット中継装置1および内部ネットワーク30を監視し、通信データの記録等を行うことによって、外部ネットワーク20から内部ネットワーク30への不正アクセス検知の手掛かりとなる情報を収集する。収集された情報は、解析装置51において解析され、ネットワーク管理者の管理者端末装置50へ通知される。

【0008】ネットワーク管理者は、管理者端末装置50を用いて、パケット中継装置1のフィルタリングテーブルを設定し、更新することができる。ネットワーク管理者は、解析装置51による解析結果に基づき、不正アクセスパケットおよび不正アクセスの疑いのあるパケットであるか否かの最終的な判断を行い、フィルタリングテーブルを変更し、不正アクセスの再発を防止している。

【0009】

【発明が解決しようとする課題】従来の侵入検知システムは上記のように構成され、ネットワーク管理者によって管理されていた。ところが、このようなネットワーク管理業務は、専門知識を有するスペシャリストのみが行うことのできる業務であるため、一部の管理者に大きな作業負荷が集中してしまうという問題があった。

【0010】また、パケット中継装置は、IDS (Intr

usion Detection System) と呼ばれる侵入検知機能を有している場合がある。IDSを用いれば、パケットデータのパターンマッチングにより、不正アクセスパケットを判別することができる。しかしながら、パケット単位のパターンマッチングだけでは不正アクセスパケットであると判断できない様な場合、内部ネットワークに不正アクセスパケットが送出されてしまうという問題があった。また、IDSによる不正アクセスパケットの検出には時間がかかるため、パケット通信量が多い場合には、全てのパケットについて判断を行うことができないという問題もあった。

【0011】本発明は、上記の事情に鑑みてなされたものであり、セキュリティ機能を有するパケット中継装置であって、不正アクセスパケット又はその疑いのあるパケットをオトリネットワークへ送出することにより、不正アクセスに対するセキュリティ性を向上させ、あるいは、不正アクセスへの対処を自動化したパケット中継装置を提供することを目的とする。また、通信量の増大時にパケットをオトリネットワークへ送出することにより、通信路の帯域を確保するパケット中継装置を提供することを目的とする。

【0012】また、セキュリティ機能を有するパケット中継システムであって、2つの中継経路を用いて、中継経路における帯域を制御し、セキュリティ性を向上させたパケット中継システムを提供することを目的とする。

【0013】また、セキュリティ機能を有するパケット中継装置および不正アクセスパケット又はその疑いのあるパケットがオトリネットワークを介して誘導されるオトリ端末装置からなるオトリ誘導システムを提供することを目的とする。さらに、セキュリティレベルを変化させ、ネットワークの監査を行い、あるいは、不正アクセスへの対処をリアルタイム化したオトリ誘導システムを提供することを目的とする。

【0014】

【課題を解決するための手段】請求項1に記載の本発明によるパケット中継装置は、第1のネットワークおよび第2のネットワーク間でパケットを中継するパケット中継部と、第1のネットワークから第2のネットワークに対して送信されたパケットを第1および第2のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを備えて構成される。

【0015】上記パケット中継部は、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、フィルタリングテーブルを用いて、第1のネットワークから第2のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、第1のネットワークから第2のネットワークに対して送信されたパケットを監視して、第2のネットワークへ不正にアクセスしよ

うとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とにより構成される。

【0016】請求項2に記載の本発明によるパケット中継装置は、オトリネットワークが、第2のネットワークと同一のアドレス体系を有するとともに、オトリ端末装置が接続される。また、オトリ誘導部が、オトリ誘導されるパケットの送信先アドレス情報に一致する第1のアドレス情報が割り当てられたオトリ端末装置に対してパケットを送出するように構成される。

【0017】請求項3に記載の本発明によるパケット中継装置は、侵入検知部が、第1のネットワークから第2のネットワークに対して送信されたパケットを所定の不正アクセスパケットのパターンデータと比較して、不正アクセスパケットを検出するように構成される。

【0018】請求項4に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリ端末装置から第1のネットワークに対して送信されたパケットをパケット中継部へ送出し、パケット中継部が、オトリ端末装置からのパケットを第1のネットワークへ送出するように構成される。

【0019】請求項5に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリネットワークに接続された汎用コンピュータにより構成され、その汎用データベースを介してパケット中継部に接続され、パケット中継部が、オトリ誘導部から受信したオトリネットワークから第1のネットワークに対して送信されたパケットに対し、フレーム形式を第2のネットワークの形式に変換して第1のネットワークに送出するように構成される。

【0020】請求項6に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリ端末装置から第1のネットワークに対して送信されたパケットについて、その送信先情報に基づき、オトリ誘導されたパケットの送信元以外を送信先とするパケットを判別し、判別されたパケットの送信元情報をオトリ端末装置に割り当てられた第2のアドレスに変更してパケット中継部へ送出するように構成される。

【0021】請求項7に記載の本発明によるパケット中継装置は、パケット中継部が、第1のネットワークから送信されるパケットについて、第2のアドレスを送信先情報とするパケットを判別し、オトリ誘導部が、判別されたパケットの送信先情報を第1のアドレスに変更して、オトリネットワークへ送出するように構成される。

【0022】請求項8に記載の本発明によるパケット中継システムは、第1および第2のパケット中継装置と、パケットを監視するパケット監視装置により構成される。第1のパケット中継装置の第1のネットワーク用のポートが第1のネットワークに接続され、第2のパケット中継装置の第1のネットワーク用のポートが第2のネットワークに接続され、第1および第2のパケット中継装置の第2のネットワーク用のポートが互いに接続さ

れ、正常パケットが伝送される第1の経路を形成し、第1および第2のパケット中継装置のオトリネットワーク用のポートが互いに接続され、監視用経路として第1のパケット中継装置によってオトリ誘導されるべきパケットが伝送される第2の経路を形成し、パケット監視装置が第2の経路に設けられる。

【0023】請求項9に記載の本発明によるオトリ誘導システムは、第1のネットワークおよび第2のネットワークに接続されたパケット中継装置と、第1および第2のネットワークとは別のオトリネットワークを介してパケット中継装置に接続されたオトリ端末装置とを備えて構成される。

【0024】上記パケット中継装置は、第1のネットワークおよび第2のネットワーク間でパケットを中継するパケット中継部と、第1のネットワークから第2のネットワークに対して送信されたパケットを第1および第2のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とにより構成される。

【0025】上記パケット中継部は、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、フィルタリングテーブルを用いて、第1のネットワークから第2のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、第1のネットワークから第2のネットワークに対して送信されたパケットを監視して、第2のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とにより構成される。

【0026】請求項10に記載の本発明によるオトリ誘導システムは、パケット中継装置が、第1のネットワークから第2のネットワークへの通信量が所定の閾値を越える場合に、第1のネットワークからのパケットをオトリ端末装置へ送出し、オトリ端末装置が、パケット中継装置からの上記パケットを記録し、第1のネットワークから第2のネットワークへの通信量の低減後に第2のネットワークに対し送信するように構成される。

【0027】請求項11に記載の本発明によるオトリ誘導システムは、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、オトリ誘導されたパケットを第2のネットワーク又は身代わり端末装置に対して送信するように構成される。

【0028】請求項12に記載の本発明によるオトリ誘導システムは、パケット中継装置が、第1のネットワークから第2のネットワークに対して送信されたパケットを第2のネットワークおよびオトリ端末装置へ送出し、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、第2ネットワークの監査を行うように構成される。

【0029】請求項13に記載の本発明によるオトリ誘導システムは、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、セッションリセットパケットを第1のネットワークに対して送出するように構成される。

#### 【0030】

【発明の実施の形態】実施の形態1. 図1は、本発明の実施の形態1によるオトリ誘導システムの一構成例を示したブロック図である。図中の1はオトリ誘導装置、2はパケット中継部、3はオトリ誘導部、4は侵入検知部、5はフィルタリング処理部、6はフィルタリングテーブル、7は内部バス、20は外部ネットワーク、21は外部端末装置、30は内部ネットワーク、31は内部端末装置、40はオトリネットワーク、41はオトリ端末装置である。

【0031】オトリ誘導装置1は、外部ネットワーク20および内部ネットワーク30に接続され、両ネットワーク間でパケット中継を行うパケット中継装置である。すなわち、外部端末装置21から内部端末装置31へのパケットを外部ネットワーク20から受信し、内部ネットワーク30へ送出する。また、内部端末装置31から外部端末装置21へのパケットを内部ネットワーク30から受信し、外部ネットワーク20へ送出する。

【0032】各ネットワーク20、30、40には、通常、2以上の端末装置が接続されているが、図中では省略されている。特に、外部ネットワーク20は、インターネットのような不特定多数の端末装置が収容されているネットワークであってもよい。オトリネットワーク40は、内部ネットワーク30には接続されてない（オトリ誘導装置1経路を除く）別個のネットワークであり、オトリ端末装置41が接続されている。

【0033】オトリ誘導装置1は、外部ネットワーク20および内部ネットワーク30に接続されたパケット中継部2と、オトリネットワーク40に接続されたオトリ誘導部3からなり、パケット中継部2およびオトリ誘導部3は、内部バス7を介して接続されている。パケット中継部2は、さらに侵入検知部4と、フィルタリング処理部5と、フィルタリングテーブル6とにより構成される。

【0034】オトリ誘導部3、侵入検知部4およびフィルタリング処理部5は、ネットワーク経路（外部ネットワーク20、内部ネットワーク30）以外のバスである内部バス7を介して互いに通信することができる。また、オトリ誘導部3および侵入検知部4は、ネットワーク中継機能を利用するユーザからは隠蔽されている。

【0035】侵入検知部4は、外部ネットワーク20からのパケットのステルス監視を行って、DoS (Denial of Service)、スキャンニングなどのネットワークレベルの攻撃（不正アクセス）を検出している。例えば、監視対象であるパケットデータを予め与えられた不正パケ

ットパターンと比較して、不正アクセスパケットを検出する。このパターンマッチングは、パケット単位だけでなく、送信元又は送信先情報によって特定される一連のパケットに対して行うこともできる。

【0036】フィルタリング処理部5は、外部ネットワーク20から送信されたパケットに対し、内部ネットワーク30への中継、オトリネットワーク40への誘導、破棄のいずれかの処理（フィルタリング処理）を行っている。この処理は、フィルタリングテーブルに基づいて行われ、例えば、内部ネットワーク30に不正にアクセスしようとする不正アクセスパケットは破棄され、不正アクセスの疑いのある被疑パケットはオトリネットワーク40へ誘導され、その他の通常パケットは、内部ネットワーク30へ送出される。

【0037】フィルタリングテーブル6には、フィルタリング処理を規定するデータが記憶されており、パケットヘッダに含まれる送信元又は送信先に関する情報と、当該パケットに対するフィルタリング処理とが関連づけられている。たとえば、破棄すべきパケットおよびオトリ誘導すべきパケットとして、パケットの送信元又は送信先情報が記憶されており、送信元又は送信先情報がフィルタリングテーブル6と一致するパケットは、破棄され、あるいは、オトリ誘導される一方、その他のパケットはネットワーク中継される。このフィルタリングテーブル6は、侵入検知部4による検出結果に基づいて更新される。

【0038】オトリ誘導部3は、内部バス7を介して、フィルタリング処理部5から、オトリ誘導すべきパケットを受信し、オトリネットワーク40上のオトリ端末装置41へ送出する。

【0039】次に動作について説明する。外部端末装置21から内部端末装置31に対して送信されたパケットは、外部ネットワーク20を介してオトリ誘導装置1により受信される。この受信パケットは、パケット中継部2のフィルタリング処理部5へ入力されるとともに、侵入検知部4にも入力される。この侵入検知部4は、パケット中継部2の入り口でプロミスカスモードかつステルスモードで通信を傍受している。

【0040】パケットを受信したフィルタリング処理部5は、フィルタリングテーブル6に基づいて、送信元又は送信先情報、例えば、送信元IP（Internet Protocol）アドレス、送信先IPアドレス、送信元TCP（Transmission Control Protocol）ポート番号、送信先TCPポート番号、送信元UDP（User Datagram Protocol）ポート番号または送信先UDPポート番号をチェックする。

【0041】この結果、フィルタリングテーブル6において、破棄の指定がされているパケットは、フィルタリング処理部5によって破棄され、オトリ誘導の指定がされているパケットがオトリサイト（オトリネットワーク

40のオトリ端末装置41）へ誘導され、ともに内部ネットワーク30には送出されない。一方、破棄および誘導等の指定がされていないパケットは内部ネットワーク30へ送出される。

【0042】図2は、図1のオトリ誘導システムにおけるパケットの流れの一例を示した図である。外部ネットワーク20から内部ネットワーク30に対して送信されたパケットは、フィルタリングテーブル6に基づいて、①破棄され、②オトリネットワーク40へオトリ誘導され、あるいは、③内部ネットワーク30へ中継される。

【0043】一方、パケットを傍受した侵入検知部4は、所定の不正アクセスパターンによりパターンマッチングを行って、傍受したパケットが不正アクセスパケットかどうかを判別する。不正アクセスパケットを受信した場合、あらかじめ定められたポリシー（不正アクセスの種類とそれに対する対策の関係）に従って、送信元又は送信先情報と、それに関連づけられるフィルタリング処理（破棄又は誘導）を決定し、内部バス7を介してフィルタリング処理部5へ通知し、フィルタリングテーブル6が更新される。

【0044】例えば、不正アクセスが疑われるパケットが検出された場合には、当該パケットがオトリ誘導の対象に追加され、不正アクセスパケットであることが検出された場合には、破棄の対象に追加される。逆に、オトリ誘導又は破棄の対象が、正常アクセスパケットであることが検出された場合には、これらの対象から除外される。このようなポリシーは予め任意に決定され、侵入検知部4に対し与えられている。

【0045】本実施の形態によれば、侵入検知部4によって外部ネットワーク20からの不正アクセスパケットが検出され、フィルタリングテーブル6が自動的に更新されるため、フィルタリングポリシーをダイナミック（動的）に自動変更させることができる。このため、不正アクセスパケットに応じた対策をリアルタイムで実現し、セキュリティ性を向上させることができる。

【0046】また、外部ネットワーク20から内部ネットワーク30へのパケットのうち、不正アクセスの疑いのあるパケットをオトリ端末装置41に誘導することによって、内部ネットワーク30への不正アクセスを未然に防止することができる。

【0047】実施の形態2。図3は、本発明の実施の形態2によるオトリ誘導システムの一構成例を示したブロック図である。図中の8はパーソナルコンピュータ、9はアドインボード、10はPCI（Peripheral Components Interconnect）バス、11はPCIインターフェース部、12はTCP/IPインターフェース部である。なお、図1に示されたブロックに相当するブロックには同一の符号を付して説明を省略する。

【0048】パーソナルコンピュータ8は、オトリ誘導部3と、PCIインターフェース部11と、TCP/IP



## 11

Pインターフェース部12からなる。オトリ誘導部3は、汎用のパーソナルコンピュータ上で実行されるソフトウェアとして構成され、PCIインターフェース部11を介してPCIバス10に接続され、アドインボード9との通信を行うとともに、TCP/IPインターフェース12を介してオトリネットワーク40に接続され、オトリ端末装置41との通信を行うことができる。このパーソナルコンピュータ8は、アドインボード9とともにオトリ誘導装置を構成する。

【0049】アドインボード9は、PCIバス10を介してパーソナルコンピュータ8に接続されたパケット中継のための機器であり、パーソナルコンピュータ8の筐体内に組み込まれている。このアドインボード9は、侵入検知部4、フィルタリング処理部5およびフィルタリングテーブル6からなり、侵入検知部4およびフィルタリング処理部5がPCIバス10に接続されている。なお、PCIバス10は、図1の内部バス7に相当し、アドインボード9は、図1のパケット中継部2に相当する。

【0050】内部ネットワーク30およびオトリネットワーク40は、パーソナルコンピュータ8およびアドインボード9を介して、PCIバスにより接続されるのみであり、ネットワークとしては両者は完全に切り離されている。このため、オトリネットワーク40の環境（例えばIPアドレス等のネットワーク設定情報）を内部ネットワーク30の環境に限りなく近づけることができる。つまり、オトリネットワーク40に、内部ネットワーク30と同じプロトコルやアドレス体系を採用し、さらに、内部ネットワーク30上の端末装置31と同じIPアドレスをオトリネットワーク40上のオトリ端末装置41に割り当てることができる。

【0051】不正アクセスを試みる外部ネットワーク20上の利用者（攻撃者）は、オトリ端末装置41との通信により、オトリ端末装置41からアクセス可能な様々な情報を取得できる可能性がある。このため、両ネットワーク30、40の環境を近づければ、不正アクセスパケットをオトリサイトに誘導した場合に、オトリ誘導していることを攻撃者に気づかれ難くすることができる。

【0052】次に動作について説明する。図4は、図3のオトリ誘導システムの通常運用時の動作の一例を示した図である。通常運用時のパケットの流れは、実施の形態1と同様にパケット中継部としてのアドインボード9を介して行われる。すなわち、①外部ネットワーク20からのパケットは、フィルタリング処理部5に入力され、破棄、オトリ誘導の対象でないパケットは、内部ネットワーク30へ送出される。②侵入検知部4は、アドインボード9の入り口でパケットを傍受し、不正アクセスかどうかの判断を行う。③不正アクセスを発見した場合、それ以降の不正アクセスを未然に防ぐために、PC

Iバスを介してフィルタリングテーブル6を更新し、中継ポリシーを自動的に変更する。

【0053】図5は、図3のオトリ誘導システムにおいて、フィルタリング処理部によってパケットがオトリ誘導される場合の動作の一例を示した図である。④外部ネットワーク20からパケットを受信したフィルタリング処理部5は、フィルタリングテーブル6に従って、送信元又は送信先情報、例えば、送信元IPアドレス、送信先IPアドレス、送信元TCPポート番号、送信先TCPポート番号、送信元UDPポート番号または送信先UDPポート番号をチェックする。この結果、オトリ誘導が指定されたパケットであれば、オトリ端末装置41へ誘導するため、当該パケットをPCIバス10を通じてパーソナルコンピュータ8へ転送する。⑤パーソナルコンピュータ上のプログラムとしてのオトリ誘導部3はパケットの種別を判断し、オトリ端末装置41が受信可能なパケット形式に変換した後、当該パケットをオトリネットワーク40へ送出する。

【0054】なお、侵入検知部4が外部ネットワーク20からの不正アクセスを検出した場合には、侵入検知部4からフィルタリング処理部5へ攻撃検知の通知が送られ、フィルタリング処理部5は内部ネットワーク30への当該通信を一旦遮断する。このとき、上述した通り、フィルタリングテーブル6が更新されるので、その後に受信した同種のパケットは、フィルタリング処理部5によってオトリ端末装置41へ誘導される。

【0055】一方、オトリ端末装置41が、外部ネットワーク20上の外部端末装置21（攻撃者）に対しパケットを送信する場合、⑥オトリ端末装置41からのパケットは、オトリネットワーク40を介してパーソナルコンピュータ8に入力される。当該パケットをTCP/IPインターフェース12を介して受け取ったオトリ誘導部3は、PCIバス10を介してアドインボード9へパケットの転送要求を出す。⑦PCIバス10を介してパケットの転送要求を受け取ったフィルタリング処理部5は、受信したパケットデータをイーサネット（登録商標）フレームの形式に変換（イーサフレーミング）して外部ネットワーク20へ送出する。

【0056】本実施の形態では、オトリ誘導部3をパーソナルコンピュータ8上のソフトウェアにより実現し、当該コンピュータにパケット中継装置としてのアドインボード9をPCIバス10により接続しているため、PCIドライバを開発すれば、既存のパーソナルコンピュータを使用して、オトリ誘導システムを構築することができる。

【0057】また、オトリ端末装置41からのパケットを外部ネットワーク20に送出し、内部ネットワーク30上の端末装置31からのパケットに見せかけているため、不正アクセスを試みる外部ネットワーク20の利用者（攻撃者）にオトリ誘導されていることを気づかれ難

くなる。

【0058】特に、オトリネットワーク40のプロトコル、アドレス体系を内部ネットワーク30のそれと同一とし、オトリ誘導される不正アクセス packets をその送信先情報（つまり内部ネットワーク上の端末装置31）と同じアドレス情報が割り当てられたオトリネットワーク40上のオトリ端末装置41に送出することにより、オトリ誘導に気づかれ難くすることができる。

【0059】実施の形態3. 実施の形態2では、オトリ端末装置41から外部ネットワーク20上の攻撃者へ packets を送信する場合について説明したが、本実施の形態では、オトリ端末装置41と、外部ネットワーク20上の攻撃者以外の端末装置との間で packets 通信を行う場合について説明する。

【0060】各オトリ端末装置41は、オトリ誘導部3により起動時に仮想的なIPアドレスが割り当てられる。オトリ誘導部3は、各オトリ端末装置41に割り当てた仮想アドレスを本来のIPアドレスに対応づけて記憶するとともに、フィルタリング処理部5に対し、仮想アドレスを通知し、これらのアドレスを送信先とした packets を受信した場合には、オトリ誘導部3に転送するように要求する。

【0061】まず、オトリ端末装置41が、外部ネットワーク20上の攻撃者以外の端末装置、たとえばDNS（Domain Name Server）に対して、 packets を送信する場合について説明する。

【0062】図6は、本発明の実施の形態3によるオトリ端末装置41から攻撃者以外の外部端末装置に packets 送信する場合の動作を示した説明図である。オトリ端末装置41には、オトリ誘導時に使用される本来のIPアドレスとして"10.255.0.1"が割り当てられ、仮想アドレスとして"10.0.0.1"が割り当てられているものとする。また、攻撃者以外の外部端末装置にはIPアドレス"w.x.y.z"が割り当てられているものとする。

【0063】オトリ誘導装置1が、オトリ端末装置41からの packets を受信した場合、オトリ誘導部3が、その packets の送信先（destination: dst）アドレスを検査して、攻撃者宛でないかを判断する。その結果、攻撃者宛でない場合には、オトリ誘導部3が当該 packets の送信元（source: src）アドレス"10.0.0.1"を、当該オトリ端末装置41に対して起動時に割り当てられた仮想アドレス"10.255.0.1"に変更する。このとき、IP packets のチェックサム（Checksum）を再計算し変更する必要がある。この様にして送信元アドレスが変更された packets は、PCIインターフェースを介してフィルタリング処理部5に送られ、オトリ誘導装置1からインターネットなどの外部ネットワーク20へ送出される。

【0064】次に、外部ネットワーク20上の攻撃者以外の端末装置、たとえばDNSからオトリ端末装置41に対して、 packets が送信される場合について説明す

る。

【0065】図7は、攻撃者以外の外部端末装置からオトリ端末装置41に対して packets 送信する場合の動作を示した説明図である。図6と同様、オトリ端末装置41には、本来のIPアドレスとして"10.255.0.1"が割り当てられ、仮想アドレスとして"10.0.0.1"が割り当てられているものとする。また、攻撃者以外の外部端末装置にはIPアドレス"w.x.y.z"が割り当てられているものとする。

【0066】オトリ誘導装置1が外部ネットワーク20から packets を受信した場合、フィルタリング処理部5は、受け取った packets の送信先アドレスが、オトリ誘導部3から予め通知された仮想アドレス"10.255.0.1"であるかを検査する。この結果、仮想アドレス宛の packets であれば、その packets をオトリ誘導部3に転送する。オトリ誘導部3は、転送された packets の送信先情報を本来のIPアドレス"10.0.0.1"に変更し、チェックサムを再計算し変更する。この様にして送信先アドレスが変更された packets は、TCP/IPインターフェース12を介してオトリネットワーク40へ送出され、オトリ端末装置41により受信される。

【0067】実施の形態4. 実施の形態1～3では、フィルタリング処理部5が受信 packets に基づいて判断し、その判断結果に基づいて、 packets をオトリ端末装置41へ送信する動作について説明したが、本実施の形態では、図1, 3のオトリ誘導システムにおいて、所定量を超える packets 通信が発生した場合に、通信 packets の全て又は一部をオトリ端末装置41に誘導する場合の動作について説明する。

【0068】図8は、本発明の実施の形態4によるオトリ誘導システムの動作の一例を示した説明図である。①通常運用時、外部ネットワーク20から受信した packets は、破棄又はオトリ誘導が指定されている packets を除き、内部ネットワーク30へ直接中継される。

【0069】一方、②予め定められた閾値を超える通信が発生した場合、フィルタリング処理部5は、全ての通信または一部の通信（たとえば、特定の送信元IPアドレス、特定の送信先IPアドレス、特定の送信元TCPポート番号、特定の送信先TCPポート番号、特定の送信元UDPポート番号または特定の送信先UDPポート番号によって限定される）をオトリ端末装置41へ誘導し、本来の通信路の帯域を確保する。このとき、オトリ端末装置41では、誘導されてきた packets をログ情報として蓄積する。

【0070】③フィルタリング処理部5から通信量が減少した旨の通知を受けたオトリ端末装置41は、蓄積しているログ情報を packets に変換して、フィルタリング処理部5へ転送する。フィルタリング処理部5は、これらの packets を内部ネットワーク30へ送出する。

【0071】本実施の形態によれば、所定の通信 packets

トを一旦、オトリ端末装置41に蓄積させることにより、特定の通信のための帯域を確保するとともに、ネットワークの負荷を分散させることができる。

【0072】実施の形態5. 実施の形態1～4では、外部ネットワークからのパケットをオトリ端末装置に誘導するオトリ誘導システムについて説明したが、本実施の形態では、これらのオトリ誘導システムにおいてオトリ誘導装置として使用されているパケット中継装置を2台連携させ、パケット中継システムとして動作させる場合について説明する。

【0073】図9は、本発明の実施の形態5によるパケット中継システムの一構成例を示した図である。図中の1A、1Bはパケット中継装置、13はパケット中継システム、14はパケット監視装置(sniffer)、15は通常ルート、16は監視ルートである。

【0074】2つの同一のパケット中継装置1A、1Bは、いずれも図1および図3においてオトリ誘導装置として示されたパケット中継装置であり、本実施の形態では、2個のパケット中継装置1A、1Bおよびパケット監視装置14によって、パケット中継システム13を構成している。

【0075】パケット中継システム13は外部ネットワーク20および内部ネットワーク30に接続され、外部ネットワーク20および内部ネットワーク30間でのパケット中継を行っている。外部ネットワーク20との接続にはパケット中継装置1Aが使用され、内部ネットワーク30との接続にはパケット中継装置1Bが使用され、両パケット中継装置1A、1Bがパケット中継システム13内で接続されている。

【0076】すなわち、外部ネットワーク側のパケット中継装置1Aは、図1、3における外部ネットワーク用ポートが、外部ネットワーク20に接続され、内部ネットワーク側のパケット中継装置1Bは、図1、3における外部ネットワーク用のポートが内部ネットワーク30に接続されている。また、パケット中継装置1A、1Bは、図1、3における内部ネットワーク用のポートが互いに接続され、中継パケットの通常ルート15を形成し、オトリネットワーク用のポートが互いに接続されて通信パケットの監視ルート16を形成している。

【0077】パケット監視装置14は、パケット中継装置1A、1B間の監視ルートに設けられ、当該ルートを通過するパケットの内容を監視している。各パケット中継装置1A、1Bを構成する図1、3におけるオトリ誘導部3は、パケットを監視ルート16へルート変更させる監視ルート誘導部となり、パケット監視装置14は誘導されたパケットのみを対象としてパケットデータを詳細にチェックし、不正アクセスパケットであるか否かを判別する。

【0078】次に動作について説明する。①通常運用時、全てのパケットが通常ルート15に割り当てられ、

監視ルート16は使用されることなく、通常ルート15経由でパケット中継が行われる。すなわち、外部ネットワーク20からのパケットは、パケット中継装置1Aにより通常ルート15へ出力され、パケット中継装置1Bを介して内部ネットワーク30へ送出される。同様にして、内部ネットワーク30からのパケットは、パケット中継装置1Bにより通常ルート15へ出力され、パケット中継装置1Aを介して外部ネットワーク20へ送出される。

10 【0079】②不正アクセスの兆候のあるパケットが検出された場合、該当するパケットには監視ルート16が割り当てられる。すなわち、パケット中継装置1A、1Bのフィルタリング処理部5が、送信元又は送信先情報に基づいて、監視ルート16に誘導すべきパケットを判別する。例えば、特定の送信元IPアドレス、特定の送信先IPアドレス、特定の送信元TCPポート番号、特定の送信先TCPポート番号、特定の送信元UDPポート番号または特定の送信先UDPポート番号により誘導すべきパケットがフィルタリングテーブルにより指定される。この様にして、判別されたパケットは、パケット中継装置1A、1Bの監視ルート誘導部(オトリ誘導部)を介して監視ルート16へ出力され、パケット監視装置14の監視対象となる。

【0080】一般に、パケット監視装置14がパケットデータを詳細にチェックしようとした場合、パケット監視装置14の負荷が増大し、処理に要する時間が長くなる。このため、パケット通信量が多い場合には、全てのパケットについてリアルタイムでチェックすることが出来なくなる。

30 【0081】本実施の形態によれば、特定のパケット、例えば不正アクセスの疑いのあるパケットのみを監視ルート16へ誘導する経路の制御を行っている。このため、パケット監視装置14は、帯域が制限された監視ルート16上のパケットについてのみ監視を行うことにより、的確なパケット監視を確実に行うことが出来る。また、不正アクセス者に気づかれることなく、物理的に隔離して監視することができる。

【0082】実施の形態6. 実施の形態1～4では、外部ネットワークからのパケットをオトリ端末装置に誘導するオトリ誘導装置について説明したが、本実施の形態では、オトリ端末装置に加えて身代わり端末装置を備え、段階的に誘導してパケットに応じてセキュリティレベルを異ならせるオトリ誘導システムについて説明する。

【0083】図10は、本発明の実施の形態6によるオトリ誘導システムの構成および動作の一例を示した図である。図中の1はパケット中継装置、20は外部ネットワーク、30は内部ネットワーク、41はオトリ端末装置、42は身代わり端末装置である。

50 【0084】①通常運用時、外部ネットワーク20から

の packets は、内部ネットワーク 30 へ直接中継される。②ある特定の通信（特定の送信元 IP アドレス、特定の送信先 IP アドレス、特定の送信元 TCP ポート番号、特定の送信先 TCP ポート番号、特定の送信元 UDP ポート番号または特定の送信先 UDP ポート番号に限定する）については、パケット中継装置 1 がオトリ端末装置 41 へ誘導する。

【0085】オトリ端末装置 41 は、受け取ったパケットについて、パケット情報を詳細に解析し、不正アクセスパケットか否かを判別する。その結果、不正アクセスパケットの可能性が低い場合には、実施の形態 4 と同様にして、当該パケットを内部ネットワーク 30 へ中継する。

【0086】一方、③不正アクセスパケットである可能性が高い場合には、身代わり端末装置 42 へ誘導する。これにより、通信の種別（送信元 IP アドレス、送信先 IP アドレス、送信元 TCP ポート番号、送信先 TCP ポート番号、送信元 UDP ポート番号または送信先 UDP ポート番号で分類される）により、セキュリティ管理のレベルを変えて管理することが可能となる。

【0087】実施の形態 7. 図 11 は、本発明の実施の形態 7 によるオトリ誘導システムの構成および動作の一例を示した図である。図中の 1 はパケット中継装置、20 は外部ネットワーク、30 は内部ネットワーク、41 はオトリ端末装置、43 はネットワーク監査装置である。

【0088】①通常運用時、外部ネットワーク 20 からの packets は内部ネットワーク 30 へ直接中継されると共に、すべての通信 packets はコピーされ、オトリ端末装置 41 へも送信される。②パケットを受け取ったオトリ端末装置 41 では、受け取ったパケット情報を解析し、特定の閾値を超える数の通信が発生していた場合、その通信情報を特定の送信元 IP アドレス、特定の送信先 IP アドレス、特定の送信元 TCP ポート番号、特定の送信先 TCP ポート番号、特定の送信元 UDP ポート番号または特定の送信先 UDP ポート番号で指定し、内部ネットワーク 30 の監査に用いる。具体的には、ネットワーク監査装置 43 上の監査プログラムから同様の packets を発生させ、内部ネットワーク 30 の抗堪性を測定する。

【0089】実施の形態 8. 図 12 は、本発明の実施の形態 8 によるオトリ誘導システムの構成および動作の一例を示した図である。オトリ端末装置 41 は、侵入検知部（不図示）を備えている。例えば、ホスト型 IDS（侵入検知プログラム）が予めインストールされている。不正アクセス packets を検出したオトリ端末装置 41 は、直ちにセッションリセット packets を送信して、外部ネットワーク 20 および内部ネットワーク 30 間での当該セッションを切断する。

【0090】次に動作について説明する。①通常運用

時、外部ネットワーク 20 からの packets は内部ネットワーク 30 へ直接中継されると共に、すべての通信はコピーされオトリ端末装置 41 へも送信される。②オトリ端末装置 41 は、パケット中継装置から受け取った packets が不正アクセスである場合、当該セッションに対しては、送信元 IP アドレス、送信先 IP アドレス、送信元 TCP ポート番号、送信先 TCP ポート番号を指定して、セッションリセット packets を送信し、セッションを切断することにより、不正アクセスにリアルタイム対処を可能とする。

【0091】

【発明の効果】本発明によれば、不正アクセスに対するセキュリティ性を向上させ、不正アクセスへの対処を自動化し、あるいは、通信量の増大時に通信路の帯域を確保することができるパケット中継装置を提供することができる。また、2つの中継経路を用いて中継経路における帯域を制御するとともにセキュリティ性を向上させたパケット中継システムを提供することができる。さらに、セキュリティ性を向上させ、セキュリティレベルを変化させ、ネットワークの監査を行い、あるいは、不正アクセスへの対処をリアルタイム化したオトリ誘導システムを提供することができる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態 1 によるオトリ誘導システムの一構成例を示したブロック図である。

【図 2】 図 1 のオトリ誘導システムにおける packets の流れの一例を示した図である。

【図 3】 本発明の実施の形態 2 によるオトリ誘導システムの一構成例を示したブロック図である。

【図 4】 図 3 のオトリ誘導システムの通常運用時の動作の一例を示した図である。

【図 5】 図 3 のオトリ誘導システムにおいて、フィルタリング処理部によって packets がオトリ誘導される場合の動作の一例を示した図である。

【図 6】 本発明の実施の形態 3 によるオトリ端末装置から攻撃者以外の外部端末装置に packets 送信する場合の動作を示した説明図である。

【図 7】 攻撃者以外の外部端末装置からオトリ端末装置 41 に対して packets 送信する場合の動作を示した説明図である。

【図 8】 本発明の実施の形態 4 によるオトリ誘導システムの動作の一例を示した説明図である。

【図 9】 本発明の実施の形態 5 によるパケット中継システムの一構成例を示した図である。

【図 10】 本発明の実施の形態 6 によるオトリ誘導システムの構成および動作の一例を示した図である。

【図 11】 本発明の実施の形態 7 によるオトリ誘導システムの構成および動作の一例を示した図である。

【図 12】 本発明の実施の形態 8 によるオトリ誘導システムの構成および動作の一例を示した図である。

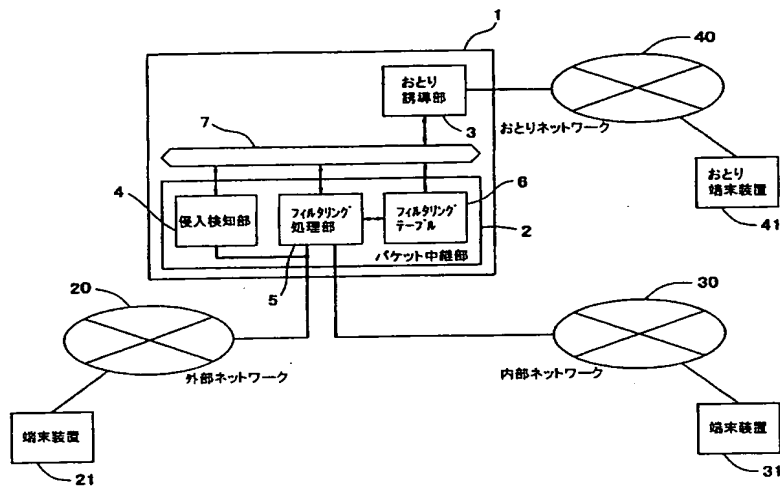
【図13】 従来の侵入検知システムの構成および動作を示した図である。

【符号の説明】

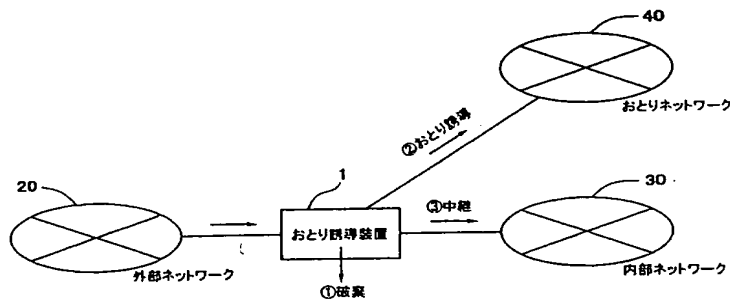
1 オトリ誘導装置（パケット中継装置）、1A、1B パケット中継装置、2 パケット中継部、3 オトリ誘導部、4 侵入検知部、5 フィルタリング処理部、6 フィルタリングテーブル、7 内部バス、8 パーソナルコンピュータ、9 アドインボード、10 PC

Iバス、11 PCIインターフェース部、12 TCP/IPインターフェース部、13 パケット中継システム、14 パケット監視装置、15 通常ルート、16 監視ルート、20 外部ネットワーク、21 外部端末装置、30 内部ネットワーク、31 内部端末装置、40 オトリネットワーク、41 オトリ端末装置、42 身代わり端末装置、43 ネットワーク監査装置、50 管理者端末装置、51 解析装置

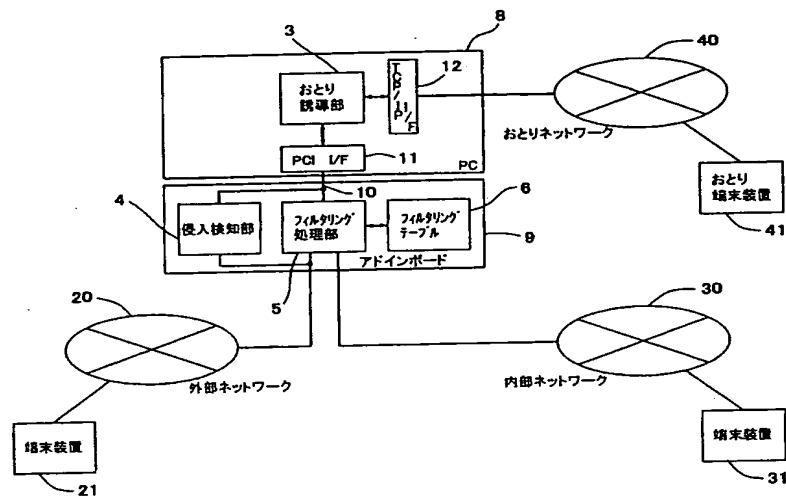
【図1】



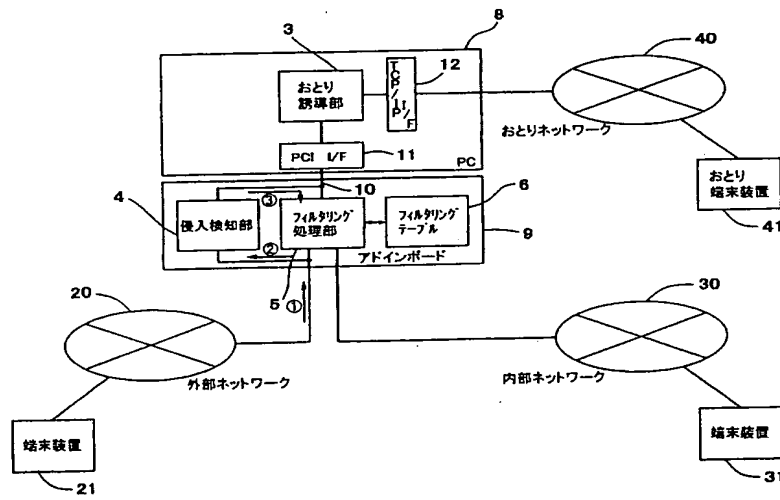
【図2】



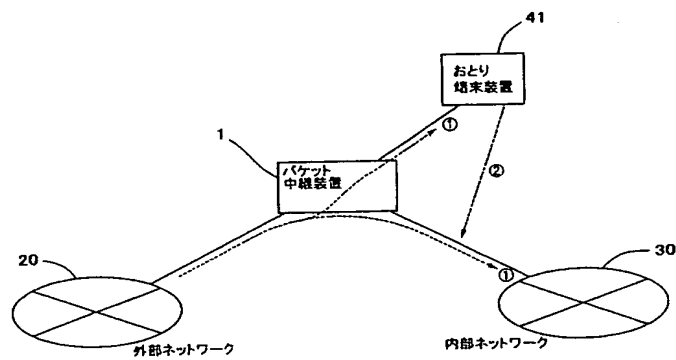
【図3】



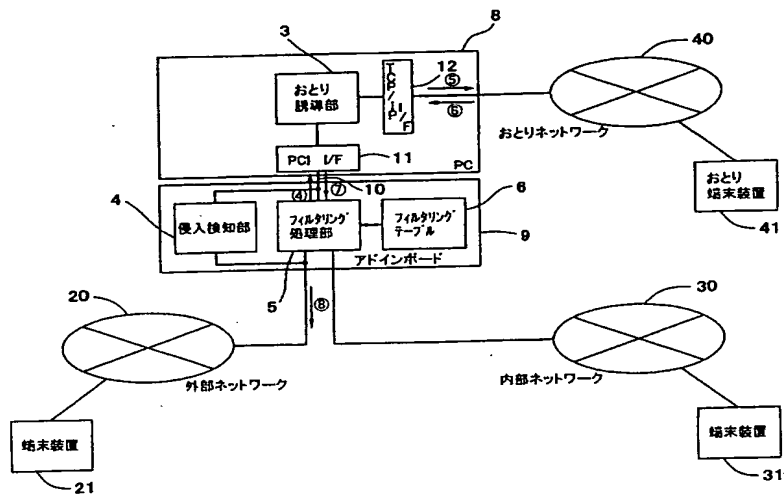
【図4】



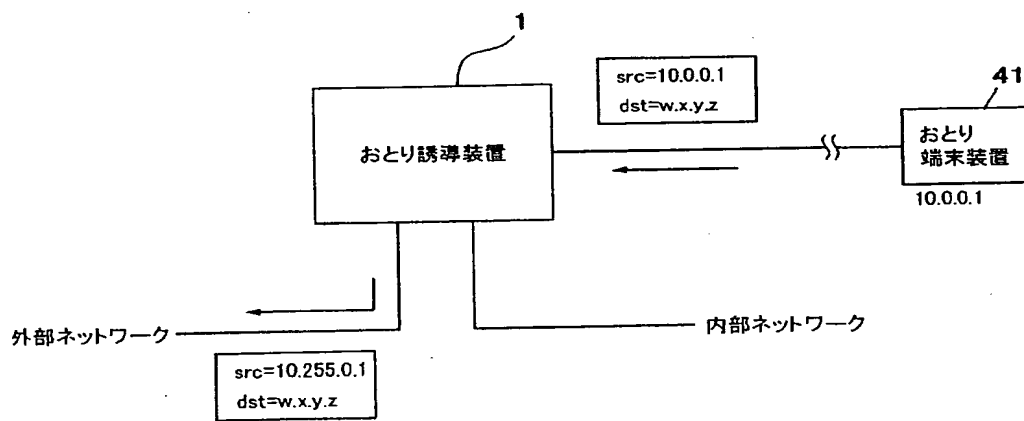
【図12】



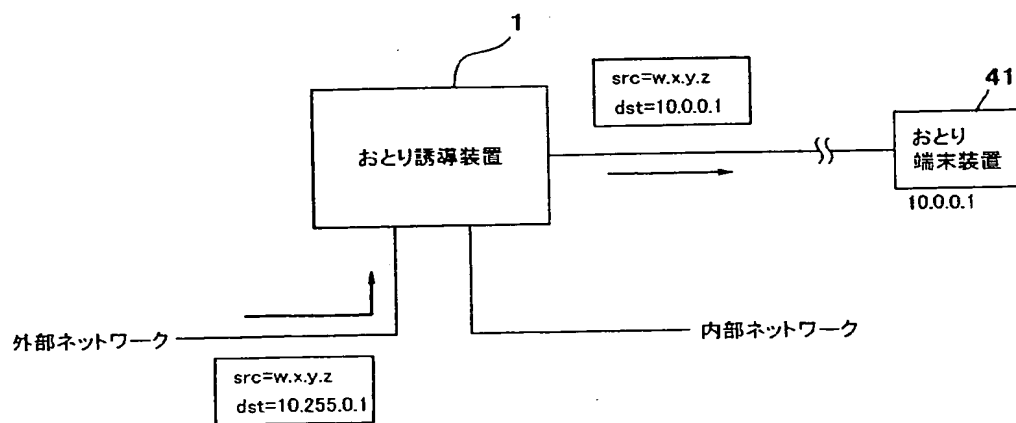
【図5】



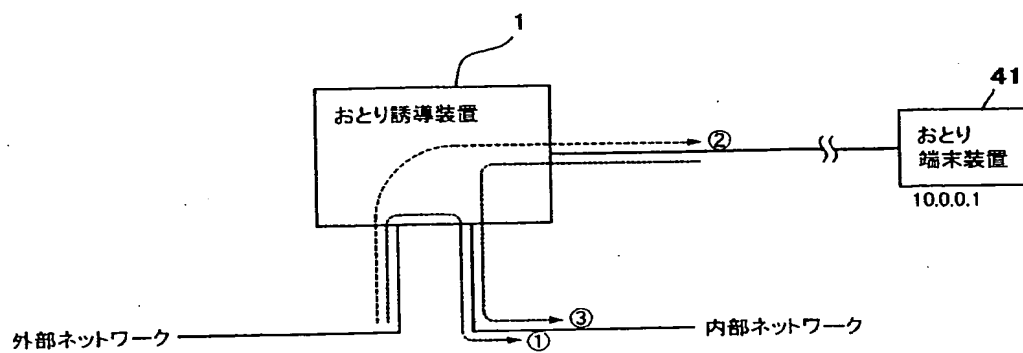
【図6】



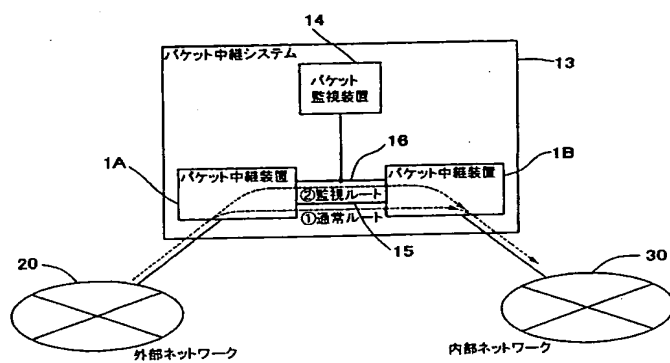
【図7】



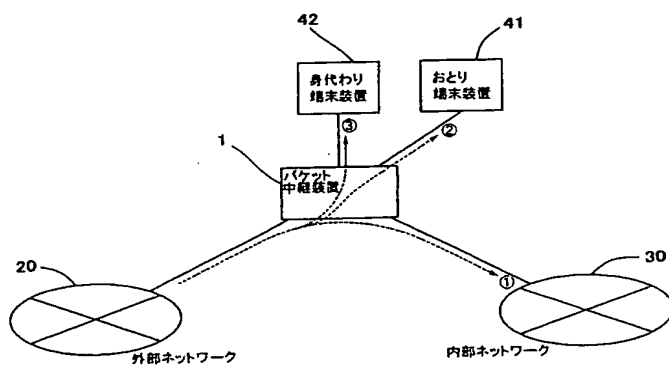
【図8】



【図9】

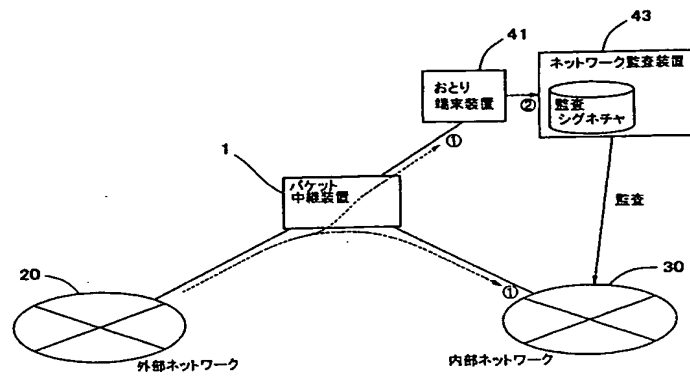


【図10】





【図11】



【図13】

